Commonwealth of Kentucky
Cabinet for Health and Family Services

Information Technology (IT) Policies

050.102 Information Systems Security Incident Response and Reporting

Version 2.0
October 14, 2015

Revision History

Date	Version	Description	Author
10/1/2006	1.0	Effective Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Revision Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Review Date	CHFS IT Policies Team Charter

Table of Contents

050.102 Information Systems Security Incident Response and Reporting

Category: 050.000 Security Awareness

1.1 Policy

Any CHFS employee who suspects an information security incident (under Employee Responsibilities) must report that incident within 1 hour of discovery to their supervisor and to the Office of Administrative and Technology Services (OATS) Office of the Executive Director. They may contact the OATS Office of the Executive Director at CHFSITSecurity@ky.gov, KHBE Security <KHBE.Security@ky.gov>, or CHFS IT Security Team on the Global Address Listing (GAL).

If any employee has questions or concerns regarding information security incidents within the Cabinet, they may contact the KHBE Security or CHFS Security as listed above.

After the conclusion of each incident, a post incident analysis report will be completed and made available for management review and action.

1.2 Scope

This policy applies to all CHFS employees and contractors, including all persons providing contractor services.

1.3 Policy/Procedure Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security and Audit Section is responsible for the maintenance of this policy.

1.4 Applicability

All CHFS employees and contractors shall adhere to the following policy.

1.5 Exceptions

There are no exceptions to this policy.

1.6 General

Office of the Executive Director follows a controlled process to log, investigate and report all security incidents. CHFS adheres to all federal requirements regarding the investigation, management and reporting of information security incidents and/or security breaches.

1.6.1 HIPAA

The Cabinet follows the HIPAA requirements for logging security incidents. Additionally, CHFS investigates potential security breaches as defined under HITECH and complies with all reporting requirements as outlined under the HITECH Act.

1.6.2 IRS Data

The Cabinet follows all security incident requirements for Federal Tax Information as outlined in IRS Publication 1075. The Cabinet reports all security incidents involving Federal Tax Information to the required contact for the IRS, no later than 24 hours after the identification of a possible incident.

1.6.3 Other

More examples of the types of incidents and breaches which could be encountered are covered in the CHFS Incident Response Plan

CHFS is committed to ensuring that the employees tasked with handling security incidents are adequately trained and prepared to handle their incident response duties. CHFS will periodically perform incident response exercises. The exercises are conducted in part as training exercises and to test the incident response process.

1.7 Employee Responsibility

CHFS employees are responsible for reporting security incidents. The following security incidents must be reported:

- Possible or actual exposure release, alteration or loss of confidential information, such as HIPAA-protected health information and federal tax information;
- Giving or telling another person your password.
- Loss or theft of a laptop or desktop computer or handheld data device.

- Loss or theft of external storage devices, like external hard drives, ZIP and flash drives, CDs and DVDs, used for Cabinet business.
- Unauthorized use of CDs, DVDs or other removable media to copy confidential information.
- Attempts to obtain HIPAA or confidential information by e-mail or other electronic communication.
- Attempts by unknown sources to persuade users to download infected e-mail or attachments.
- Receipt of unsolicited, unusual or suspicious e-mail or phone calls.
- Unauthorized physical entry into a controlled area that contains confidential or HIPAA-protected information.
- Electronic monitoring of another employee's workstation.
- Blackberry password disabled.

When a security incident is related to federal tax information, CHFS will notify the Internal Revenue Service (IRS) and all required staff. The points of contact with the IRS are:

Special Agent-in-Charge, Treasury Inspector General for
Tax Administration (TIGTA)
Chicago, IL
(312) 886-0620
&
IRS Office of Safeguards
safeguardreports@irs.gov

1.8 Definitions

Security Breach:

- The unauthorized acquisition, distribution, disclosure, or release of unencrypted or unredacted records or data that compromises the security, confidentiality, or integrity of personal information (see CHFS IT Policy #010.105 for definition).
- The unauthorized acquisition, distribution, disclosure, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data.

1.9 Management Commitment

This policy has been approved by OATS Division Directors, the OATS Executive Director, and the Office of Policy and Budget out of the Office of the Secretary. Senior Management supports the objective put into place by this policy.

1.10 Review Cycle

Annual

1.11 Cross Reference(s)

- CHFS IT Policy #010.102 – Data Media Security
- CHFS IT Policy #070.203 – Exceptions to Standards and Policies.
- CHFS OHRM Personnel Handbook
- CHFS 219 Confidentiality Agreement
- Enterprise IT Policy: CIO-085 -- Agency Security Contact
- Enterprise IT Policy: CIO-090 - Information Security Incident Response Policy
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- KHBE Incident Response Plan
- National Institute of Standards and Technology (NIST) Special Publications (SP) document SP-800-30 – Risk Management Guide for Information Technology Systems